IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: White, Newton	
Serial Number: 09/682,985	Group Art Unit: 2135
Filing Date: November 5, 2001	Examiner: Son, Linh LD
Title: Exchange Method and Apparatus	Conf. No.: 4151
Attorney Docket Number: GREN.P-001-2	

RESPONSE TO OFFICE ACTION

Dear Sir:

The following paper responds to the Office Action mailed March 20, 2006 (hereinafter, the Office Action).

REMARKS/ARGUMENTS

Claim Rejections - 35 USC Section 103(a)

The **First Issue** is whether the Examiner is justified in rejecting claims 1-3 under 35 USC 103(a) as being unpatentable over Rich Casselberry et al, (http://www.docs.rinet.ru/PerfectIntranet/index.htm), hereinafter "Casselberry", despite: (1-a) Casselberry's failure to disclose (1-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, (1-a-2) configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, and (1-a-3) configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443; (1-c) the fact that (1-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP), (1-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results, (1-c-3) for several years after Applicant first reduced Applicant's invention to practice and for several years since Casselberry was written, others who are skilled in the art did not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem as defined below at 1-c (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443), and (1-c-4) the Examiner failed to describe modifications to Casselberry that in the view of the examiner both (i) would bring Casselberry within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Casselberry and was confronted by the Firewall Problem; and (1-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

To understand the following discussion, it is useful to remember that when a web browser program running on a client computer sends to a web host computer a packet requesting a new session, the sent packet typically includes, among other things, a destination port number. The destination port number is the port number where the client

computer hopes the host will be listening for session requests of the type that the client computer is making in the sent packet.

Normally, if the client computer wishes to establish a HTTP session with the host, the client computer will specify a Destination Port of 80. Note that for many browser programs a URL of the form http://www.domain.com implies port 80 and is equivalent to a URL of the form http://www.domain.com:80.

Normally, if the client computer wishes to establish a HTTPS session with the host, the client computer will specify a Destination Port of 443. Note that for many browser programs a URL of the form https://www.domain.com implies port 443 and is equivalent to a URL of the form https://www.domain.com:443.

One embodiment of Applicant's invention concerns configuring a web server to listen for requests for HTTPS sessions on port 80 (rather than port 443) and then directing a web browser to send requests for HTTPS sessions to port 80 (rather than port 443), thereby permitting encrypted communications through firewalls near the client computer that block communication to ports other than port 80. For example, by directing a browser to request a URL of the form https://www.domain.com:80.

(1-a) Casselberry's failure to disclose required elements of claims 1-3.

(1-a-1) Casselberry fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number normally associated with a hypertext transfer protocol, as required by Claim 1 step (a) (upon which claims 2-3 depend).

Applicant has repeatedly admitted that at the time of Applicant's invention it was well known by those skilled in the art how to configure an HTTPS server to listen for requests for https sessions on any desired port. See for example the Application as

published at page 12 paragraphs 0239-0242 which included instructions for configuring an https server to listen on port 80.

Consequently, there is no need for the Examiner to produce any further references or evidence to prove that at the time of Applicant's invention it was well known by those skilled in the art how to configure an HTTPS server to listen for requests for https sessions on any desired port. Thus, the discussion in the Office Action at page 4, lines 12-21 does not advance the Examiner's argument. In addition, there is no need for the Examiner to bother searching for additional references which prove that at the time of Applicant's invention it was well known by those skilled in the art how to configure an HTTPS server to listen for requests for https sessions on any desired port. The Examiner won this point when Applicant filed the Application.

The crucial issue for claims 1-3 is whether, at the time of Applicant's invention, it would have been obvious to one skilled in the art, when confronted with the Firewall Problem, to configure an HTTPS server to listen for requests on a port normally associated with an HTTP server. The Examiner's position is like arguing that a reference which discloses the art of sand casting renders obvious all articles that can be made using sand casting.

If the Examiner wishes to argue that it would be obvious to make the leap from "an HTTPS server can listen on any port" to "an HTTPS server ought to be configured to listen on the port normally associated with an HTTP server", there is no need for the Examiner to cite any additional support for the proposition (already admitted to be true by Applicant) that it was well known at the time of Applicant's invention how to configure an HTTPS server to listen on any port. The Examiner need only cite a reference which recommends that an HTTPS server be configured to listen on port 80.

Applicant has carefully examined the portions of the Office Action that address claims 1-3 and has been unable to find therein any discussion of any evidence supporting the position that at the time of Applicant's invention it would have been obvious to one skilled in the art (who presumably would have known how to configure any server to

listen on any port), to configure an HTTPS server to listen on the port normally associated with an HTTP server.

Applicant, to the contrary, continues to believe that configuring an HTTPS server to listen on port 80 was non-obvious at the time of Applicant's invention, even to one skilled in the art who knew that an HTTPS server could be configured to listen on any port.

Applicant contends that if, at the time of Applicant's invention, a programmer skilled in the art had encountered difficulty communicating from a browser program, through a firewall that blocked access to ports other than 80, to an HTTPS server listening on port 443, it would not have been obvious for such a programmer to (i) start with Casselberry, (ii) decide that Casselberry offers some sort of help solving the problem (for goodness knows what reason), and (iii) finally, configure the HTTPS server to listen on port 80.

(1-a-2) Casselberry fails to disclose configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, as required by Claim 2. Since HTTPS is an example of a secure hypertext transport protocol and HTTP is an example of a Hypertext Transport Protocol, the general discussion above for item 1-a-1 is fully applicable here.

(1-a-3) Casselberry fails to disclose configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443, as required by Claim 3. Since HTTPS is an example of a secure hypertext transport protocol that normally uses port 443 and HTTP is an example of a Hypertext Transport Protocol that normally uses port 80, the general discussion above for item 1-a-1 is fully applicable here.

(1-c) As discussed in the Application as published on page 12 paragraphs 0232 – 0236, Applicant's invention seeks to solve the following problem (the "Firewall

Problem"): how can a client computer use HTTPS to communicate securely with a server computer when such client computer is connected to the Internet through a firewall that blocks packets addressed to destination port 443 (the port number normally associated with HTTPS) but passes packets addressed to destination port 80.

The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem.

(1-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP).

A. The materials available at http://ftp.monash.edu.au/pub/ap/Apache/ch01.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch04.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch05.htm, http://ftp.monash.edu.au/pub/ap/Apache/ch07.htm (hereinafter, collectively, "Apache Manual"), copies of which have already been provided by the Examiner and/or the Applicant, teach away from using port 80 for any protocol other than http and teach away from using ports 1-1024 as a nonstandard port for a server.

In Chapter 1 of Apache Manuals at Fig. 1.1 (page 3 of 11 when printed by Applicant), the www service (which uses http, the hyper text transfer protocol) is equated with port 80. This teaches away from the notion that port 80 should be used for other protocols, including without limitation SSL/https.

In Chapter 7 of Apache Manuals under the heading "Protecting Your Data from Outside Access" at "Caution" (which appears on page 29 of 38 when printed by Applicant), in the context of discussing how to hide a non-secure/http server, says in relevant part:

"The second way to make your server less likely to be found is to run it on a nonstandard port. Ports can range from 0 to 65,535, so there is a wide range to choose from. Generally, the first 1024 are considered reserved ports."

By pointing out how many ports are potentially available and observing that the first 1024 are considered reserved ports, Apache teaches away from moving any server to a non-standard port in the range from 0 to 1024. That range includes port 80 which is normally associated with HTTP / hyper text transfer protocol.

B. The Applicant previously filed a copy of Running a Perfect Web Site with Windows – Chapter 5, hereinafter "Windows (Chapter 5)" (from the web at http://www.gsu.unibel.by/pub/perf_web/06r07632.HTM).

The notice at the top of Windows (Chapter 5) says "Copyright © 1996" and is very similar to the notice at the top of Chapter 4 of Apache that was provided by the Examiner.

Windows (Chapter 5) at the bottom of page 3 says in relevant part:

"… Ports under 1024 are reserved for the most common types of Internet traffic, so it is recommended that you use a number above 1024 if you need an alternate port. …"

(1-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. At the time of Applicant's invention, based upon materials such as Apache Manuals and Windows (Chapter 5), one skilled in the art would have expected that changing the port number on which an HTTPS server listens for session requests would make it harder for clients to communicate with such server. However, for clients connected to the Internet through certain types of firewalls, configuring an HTTPS server to listen on port 80 can make it possible for a client to establish an HTTPS session with such server in circumstances where it would not have been possible to establish an HTTPS session with such server if it were listening on port 443, the default port for HTTPS.

It is unexpected, serendipitous and counter-intuitive that configuring a server to listen to a non-standard and unexpected port would make it easier for some clients to reach such server, since this is precisely the sort of change that Apache and Windows (Chapter 5) teaches will make it harder for browsers to communicate with the server.

The unexpected, serendipitous and counter-intuitive results obtained by practicing the Applicant's invention cut strongly against the Examiner's view that Applicant's invention was obvious at the time it was made.

(1-c-3) During the years that have passed since Applicant first reduced Applicant's invention to practice and the years that have passed since Casselberry was written, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443).

By rejecting Applicant's invention as obvious, the Examiner (in essence) contends that, at the time of Applicant's invention, it would have been obvious to one skilled in the art, when faced with the Firewall Problem addressed by Applicant's invention (i.e., that some clients are unable to communicate with a web server using HTTPS because such clients are connected to the Internet through a firewall that blocks packets to destination port 443), to configure the destination web server to listen for requests for HTTPS sessions on port 80 and to direct the affected clients' browsers to request information using a resource locator of the form "https://www.domain.com:80".

The technical staff of every e-commerce web site that attempts to do business with the general public ought eventually to encounter the Firewall Problem since some customers and some potential customers spend some time at offices or other locations where their computers are connected to the Internet through firewalls that block outgoing packets addressed to destination port 443.

Consequently, if Applicant's invention should have been obvious to anyone skilled in the art who encountered the Firewall Problem, then it would be logical to expect that the technical staffs of many e-commerce web sites that seek to do business with the general public would either (i) have duplicated Applicant's invention or (ii) have settled upon some other solution to the Firewall Problem that permits secure communication with affected customers' computers.

However, as of December of 2005, several years after the application was filed, Applicant was not personally aware of any web sites that directed a customer's browser to a resource locator of the form https://www.domain.com:80 or implemented some other solution to the Firewall Problem that permits secure communication with customers' computers that are affected by the Firewall Problem.

Consider for example the web sites barnesandnoble.com and amazon.com – two popular, highly competitive, technologically savvy e-commerce web sites that seek to conduct business with the general public -- as they existed in December of 2005.

Based on tests conducted by Applicant on December 13, 2005, it appears that at such time, when confronted with the Firewall Problem, the persons skilled in the art employed by barnesandnobel.com decided to drop back and punt. To ensure security, barnesandnobel.com used SSL (i.e., HTTPS) for order submission and the collection of credit card information. At that time, if the computer used by a potential customer of barnesandnobel.com was connected to the Internet through a firewall that blocked outgoing packets addressed to destination port 443, then the potential customer was allowed to fill up a shopping cart but at checkout time the potential customer's browser would display an unhelpful error message as soon as the customer's browser was directed to establish an HTTPS session using the default destination port of 443.

Based on tests conducted by Applicant on December 13, 2005, it was clear that when confronted with the Firewall Problem, the persons skilled in the art employed by amazon.com had also failed to duplicate Applicant's invention or to implement some

different solution that permitted encrypted communication with affected customers. The folks at amazon.com clearly recognized the Firewall Problem, warned customers about it, and offered affected customers the choice of giving up or submitting order and payment details in an unsecured manner (i.e., using HTTP rather than HTTPS).

In particular, the last page of the checkout process that amazon.com normally sent to customers at that time without encryption (i.e., using HTTP) contained both a button labeled:

"Sign in using our secure server"and a link that said :"The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server."

If a customer should have clicked on the button labeled "Sign in using our secure server", then such customer's browser would have been directed to a URL of the form "https://www.amazon.com/*", which by default implies destination port 443. If such customer's computer should have been connected to the Internet through a firewall that blocked outgoing packets addressed to destination port 443 and such customer should have clicked on such button, then such customer would have seen an uninformative error message.

If a customer should have clicked on the "standard server" link, then such customer's browser would have been directed to a URL of the form "http://www.amazon.com/*" which by default implies destination port 80, thereby avoiding part of the Firewall Problem. Unfortunately, since that URL begins with "http", the remainder of the checkout process, including the transmission of credit card information, would then have been conducted using HTTP which is NOT encrypted for security.

Since as of December 2005, several years after the application was filed, popular e-commerce sites that sought to do business with the general public neither (i) routinely used URLs of the form "https://www.securedomain.com/*:80" for the secure portions of

their check out procedures nor (ii) routinely used some other solution to the Firewall Problem that ensured secure, encrypted communications with affected customers' computers, Applicant contends that Applicant's invention was not obvious when it was first reduced to practice by Applicant and remained non-obvious several years later.

(1-c-4) The Examiner failed to describe modifications to Casselberry that in the view of the examiner both (i) would bring Casselberry within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Casselberry and was confronted by the Firewall Problem.

As a matter of logic, no matter how many references show that a server can be associated with a non-standard port, if no reference discloses associating a server with a port that is normally associated with some other server, then no combination of such references discloses associating a server with a port that is normally associated with some other server.

(1-d) The Examiner has failed to provide any prior art to support a view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Casselberry in a way that would bring Casselberry within the scope of any of Claims 1-3. Applicant disagrees with the Examiner's view that it would be obvious to one of ordinary skill in the art to modify Casselberry in a way that would bring Casselberry within the scope of any of Claims 1-3. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges the Examiner's view and asks whether the Examiner can (i) describe a modification to Casselberry that would bring Casselberry within the scope of Claims 1-3 and (ii) show support for the view that it would have been obvious at the time of Applicant's invention for one skilled in the art so to modify Casselberry upon encountering the Firewall Problem.

In light of the foregoing discussion, Applicant respectfully requests that claims 1-3 be allowed.

The **Second Issue** is whether the Examiner is justified in rejecting Claim 4 under 35 USC 103(a) as being unpatentable over Casselberry, despite:
(2-a) Casselberry's failure to disclose (2-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (2-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol;
(2-c) the fact that (2-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP), (2-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results, (2-c-3) during the several years between when Applicant first reduced Applicant's invention to practice and December of 2005 and the several years since Casselberry was written and December of 2005, others who are skilled in the art did <u>not</u> regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem and (2-c-4) the Examiner failed to describe modifications to Casselberry that in the view of the examiner both (i) would bring Casselberry within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Casselberry and was confronted by the Firewall Problem; and (2-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(2-a) Casselberry fails to disclose elements of claim 4.

(2-a-1) Casselberry fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 step (a), upon which Claim 4 depends. See the detailed discussion above at (1-a-1).

(2-a-2) Casselberry fails to disclose receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it

were addressed to the port number associated with a secure hypertext protocol, as required by Claim 1 step (b) and Claim 4.

Applicant has been unable to figure out how the cited portions of Casselberry, which teach about changing the port on which a server listens for packets, can be viewed as disclosing anything about (i) a system that might block a packet if various conditions were satisfied or (ii) sending a packet through such a system on its way to an HTTPS server.

(2-c) The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(2-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(2-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-2.

(2-c-3) During the years between when Applicant first reduced Applicant's invention to practice and December of 2005 and the years between when Casselberry was written and December of 2005, others who are skilled in the art did not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(2-c-4) The Examiner failed to describe modifications to Casselberry that in the view of the examiner both (i) would bring Casselberry within the scope of Claim 4 and (ii) would have been obvious to one skilled in the art who was aware of Casselberry and was confronted by the Firewall Problem. See the discussion at 1-c-4.

(2-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Casselberry to include, in combination, all of the elements of claim 4 that are missing from Casselberry, including, inter alia: (2-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (2-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext transfer protocol. Furthermore, the Examiner has failed to set forth modifications to Casselberry that would bring Casselberry within the scope of Claim 4. Applicant disagrees with the view that it would have been obvious to modify Casselberry in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Casselberry that would bring Casselberry within the scope of Claim 4.

In light of the foregoing discussion, Applicant respectfully requests that Claim 4 be allowed.

The **Third Issue** is whether the Examiner is justified in rejecting Claim 5-9 under 35 USC 103(a) as being unpatentable over Casselberry. Each of Claims 5-9 is dependent (directly or indirectly) from Claim 1. Consequently Each of Claims 5-9 is patentable if Claim 1 is patentable.

For the reasons set forth above with respect to Claim 1, Applicant respectfully requests that Claims 5-9 be allowed.

The **Fourth Issue** is whether the Examiner is justified in rejecting claims 10-11 under 35 USC 103(a) as being unpatentable over Casselberry, despite:
(4-a) Casselberry's failure to disclose (4-a-1) configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443;

(4-c) the fact that (4-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP), (4-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results, (4-c-3) for several years after Applicant first reduced Applicant's invention to practice and for several years since Casselberry was written, others who are skilled in the art did not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem as defined at 1-c (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443), and (4-c-4) the Examiner failed to describe modifications to Casselberry that in the view of the examiner both (i) would bring Casselberry within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Casselberry and was confronted by the Firewall Problem; and

(4-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(4-a) Casselberry's failure to disclose required elements of claims 10-11.

(4-a-1) Casselberry fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on port 80 as required by Claim 10 step (a) and Claim 11 element (a). See the discussion above at 1-1-1.

Applicant has repeatedly admitted that at the time of Applicant's invention it was well known by those skilled in the art how to configure an HTTPS server to listen for requests for https sessions on any desired port. Consequently, there is no need for the Examiner to produce any further references or evidence to prove that at the time of Applicant's invention it was well known by those skilled in the art how to configure an HTTPS server to listen for requests for https sessions on any desired port. Thus, the discussion in the Office Action at pages 6-7, paragraph 10 does not advance the Examiner's argument. In addition, there is no need for the Examiner to bother searching for additional references which prove that at the time of Applicant's invention it was well known by those skilled in the art how to configure an HTTPS server to listen for requests

for https sessions on any desired port. The Examiner won this point when Applicant filed the Application.

The crucial issue for claims 10-11 is whether, at the time of Applicant's invention, it would have been obvious to one skilled in the art (who presumably would have known that an HTTPS server could be configured to listen on any port), when confronted with the Firewall Problem, to configure an HTTPS server to listen for requests on port 80. The Examiner's position is like arguing that a reference which discloses the art of sand casting would render obvious all articles that can be made using sand casting.

If the Examiner wishes to argue that it would be obvious to make the leap from "an HTTPS server can listen on any port" to "an HTTPS server ought to be configured to listen on port 80", there is no need for the Examiner to cite any additional support for the proposition (already admitted to be true by Applicant) that it was well known at the time of Applicant's invention how to configure an HTTPS server to listen on any port.

Applicant has carefully examined the portions of the Office Action that address claims 10-11 and has been unable to find therein any discussion of any evidence supporting the position that at the time of Applicant's invention it would have been obvious to one skilled in the art, who knew how to configure any server to listen on any port, to configure an HTTPS server to listen on port 80.

Applicant, to the contrary, continues to believe that configuring an HTTPS server to listen on port 80 was non-obvious at the time of Applicant's invention, even to one skilled in the art who knew that an HTTPS server could be configured to listen on any port.

Applicant contends that if, at the time of Applicant's invention, a programmer skilled in the art had encountered difficulty communicating from a browser program, through a firewall that blocked access to ports other than 80, to an HTTPS server listening on port 443, it would not have been obvious for such a programmer to (i) start with Casselberry, (ii) decide that Casselberry offers some sort of help solving the

problem (for goodness knows what reason), and (iii) configure the HTTPS server to listen on port 80.

(4-c) The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem.

(4-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See discussion at 1-c-1.

(4-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-2.

(4-c-3) During the years between when Applicant first reduced Applicant's invention to practice and December of 2005 and the years between when Casselberry was written and December of 2005, others who are skilled in the art did not regularly and routinely duplicate Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(4-c-4) The Examiner failed to describe modifications to Casselberry that in the view of the examiner both (i) would bring Casselberry within the scope of Claims 10 and 11 and (ii) would have been obvious to one skilled in the art who was aware of Casselberry and was confronted by the Firewall Problem. See the discussion at 1-c-4.

(4-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Casselberry to include, in combination, all of the elements of claims 10 and 11 that are missing from Casselberry, including, inter alia: (4-a-1) configuring a server program to listen for requests for HTTPS sessions on port 80. Furthermore, the Examiner has failed to set forth modifications to Casselberry that would bring Casselberry within

the scope of Claim 10 or 11. Applicant disagrees with the view that it would have been obvious to modify Casselberry in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Casselberry that would bring Casselberry within the scope of Claims 10 and 11.

In light of the foregoing discussion, Applicant respectfully requests that Claims 10 and 11 be allowed.

Preemptive Strike

As discussed above, Applicant has consistently admitted that at the time of Applicant's invention it was well known by those skilled in the art how to associate an HTTPS server with any port number. If the Examiner continues to believe that Applicant's invention is obvious in light of that fact, then perhaps the next step should be a final action and an appeal rather than further searches for references that disclose something which Applicant already admits was well known by those skilled in the art at the time of Applicant's invention.

Respectfully submitted,

_____/s/_____
Carl Oppedahl
Attorney for Applicant
Reg. No. 32746
P.O. Box 4850
Dillon, CO 80443-4850
Telephone 970-468-8600